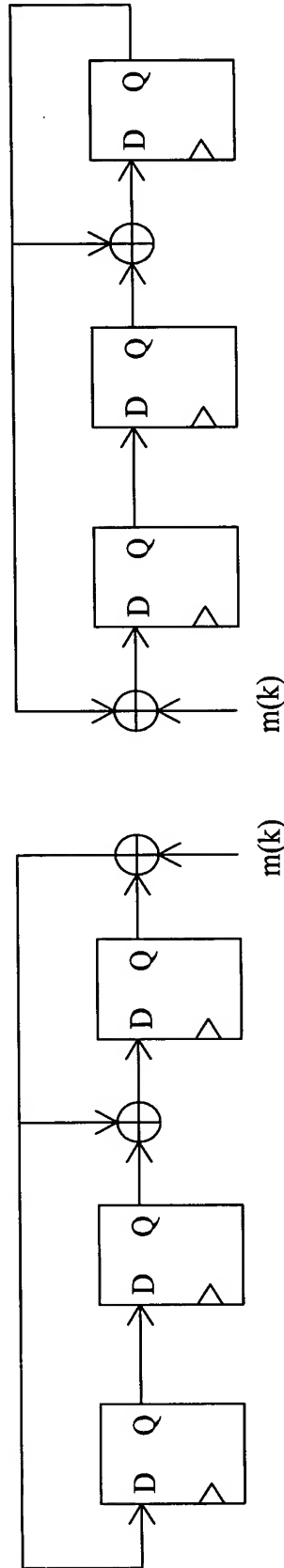


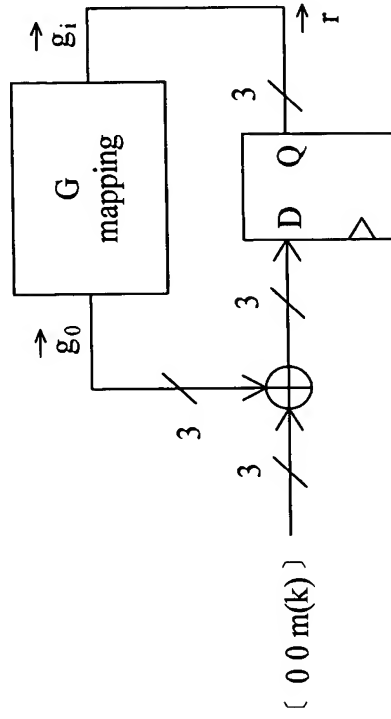
$$g(x) = x^3 + x^2 + 1$$



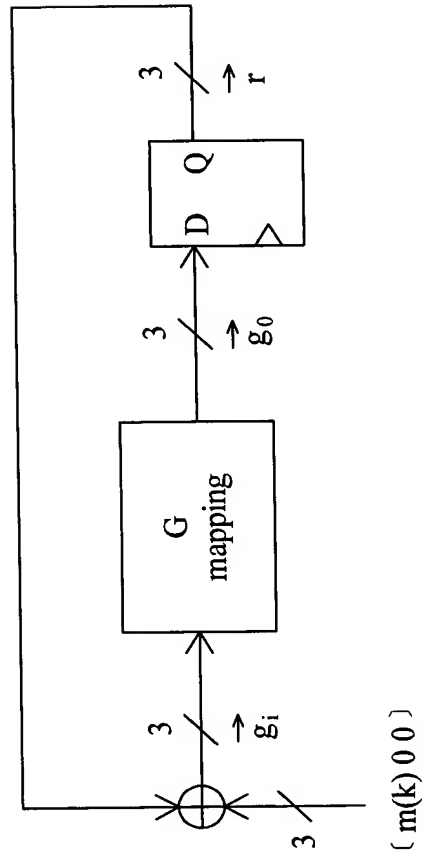
Scheme 2

Scheme 1

Fig. 1



Scheme 2

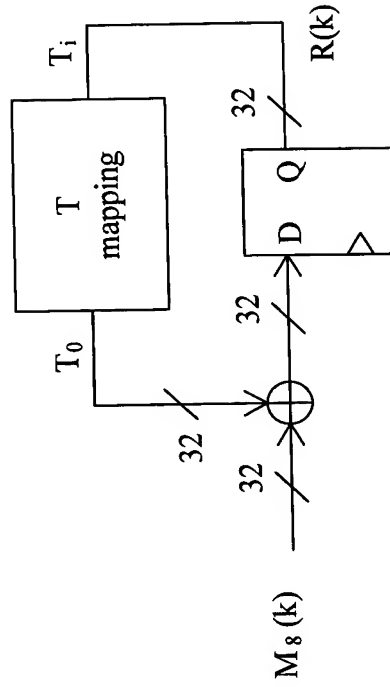


Scheme 1

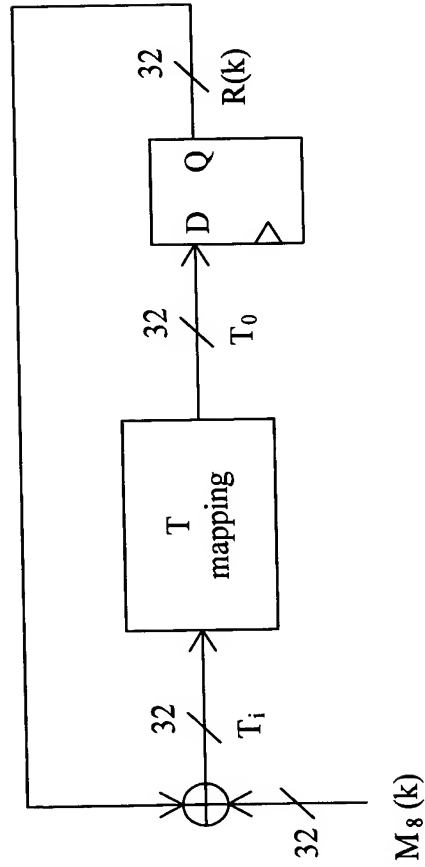
Fig. 2

| | | | | | |
|-----|-------|------------|-------------------|-------|------------|
| G = | Row31 | 0x40000000 | G ⁻¹ = | Row31 | 0x00000001 |
| | Row30 | 0x20000000 | | Row30 | 0x80000000 |
| | Row29 | 0x10000000 | | Row29 | 0x40000000 |
| | Row28 | 0x08000000 | | Row28 | 0x20000000 |
| | Row27 | 0x04000000 | | Row27 | 0x10000000 |
| | Row26 | 0x82000000 | | Row26 | 0x08000000 |
| | Row25 | 0x01000000 | | Row25 | 0x04000001 |
| | Row24 | 0x00800000 | | Row24 | 0x02000000 |
| | Row23 | 0x80400000 | | Row23 | 0x01000000 |
| | Row22 | 0x80200000 | | Row22 | 0x00800001 |
| | Row21 | 0x00100000 | | Row21 | 0x00400001 |
| | Row20 | 0x00080000 | | Row20 | 0x00200000 |
| | Row19 | 0x00040000 | | Row19 | 0x00100000 |
| | Row18 | 0x00020000 | | Row18 | 0x00080000 |
| | Row17 | 0x00010000 | | Row17 | 0x00040000 |
| | Row16 | 0x80008000 | | Row16 | 0x00020000 |
| | Row15 | 0x00004000 | | Row15 | 0x00010001 |
| | Row14 | 0x00002000 | | Row14 | 0x00008000 |
| | Row13 | 0x00001000 | | Row13 | 0x00004000 |
| | Row12 | 0x80000800 | | Row12 | 0x00002000 |
| | Row11 | 0x80000400 | | Row11 | 0x00001001 |
| | Row10 | 0x80000200 | | Row10 | 0x00000801 |
| | Row9 | 0x00000100 | | Row9 | 0x00000401 |
| | Row8 | 0x80000080 | | Row8 | 0x00000200 |
| | Row7 | 0x80000040 | | Row7 | 0x00000101 |
| | Row6 | 0x00000020 | | Row6 | 0x00000081 |
| | Row5 | 0x80000010 | | Row5 | 0x00000040 |
| | Row4 | 0x80000008 | | Row4 | 0x00000021 |
| | Row3 | 0x00000004 | | Row3 | 0x00000011 |
| | Row2 | 0x80000002 | | Row2 | 0x00000008 |
| | Row1 | 0x80000001 | | Row1 | 0x00000005 |
| | Row0 | 0x80000000 | | Row0 | 0x00000003 |

Fig. 3



Scheme 2



Scheme 1

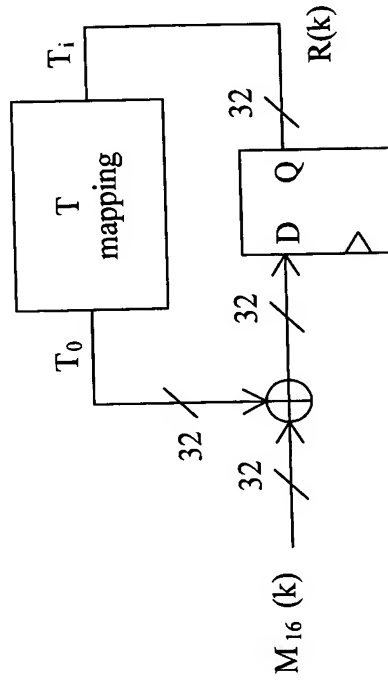
Fig. 4

| | | | |
|---------------------|-------|------------|---|
| $T = G^8 =$ | Row31 | 0x20800000 | 2 |
| | Row30 | 0x90400000 | 3 |
| | Row29 | 0xc8200000 | 4 |
| | Row28 | 0x64100000 | 4 |
| | Row27 | 0xb2080000 | 5 |
| | Row26 | 0x59040000 | 5 |
| | Row25 | 0x0c020000 | 3 |
| | Row24 | 0x86010000 | 4 |
| | Row23 | 0x43008000 | 4 |
| | Row22 | 0x01004000 | 2 |
| | Row21 | 0x20002000 | 2 |
| | Row20 | 0x10001000 | 2 |
| | Row19 | 0x88000800 | 3 |
| | Row18 | 0xc4000400 | 4 |
| | Row17 | 0x62000200 | 4 |
| | Row16 | 0x31000100 | 4 |
| | Row15 | 0xb8000080 | 5 |
| | Row14 | 0xdc000040 | 6 |
| | Row13 | 0xee000020 | 7 |
| | Row12 | 0x77000010 | 7 |
| | Row11 | 0x1b000008 | 5 |
| | Row10 | 0x2d000004 | 5 |
| | Row9 | 0x36000002 | 5 |
| | Row8 | 0x1b000001 | 5 |
| | Row7 | 0xad000000 | 5 |
| | Row6 | 0xf6000000 | 6 |
| | Row5 | 0xfb000000 | 7 |
| | Row4 | 0x5d000000 | 5 |
| | Row3 | 0x8e000000 | 4 |
| | Row2 | 0xc7000000 | 5 |
| | Row1 | 0xc3000000 | 4 |
| | Row0 | 0x41000000 | 2 |
| $T^{-1} = G^{-8} =$ | Row31 | 0x000000d5 | 5 |
| | Row30 | 0x0000006a | 4 |
| | Row29 | 0x00000035 | 4 |
| | Row28 | 0x0000001a | 3 |
| | Row27 | 0x0000000d | 3 |
| | Row26 | 0x00000006 | 2 |
| | Row25 | 0x000000d6 | 5 |
| | Row24 | 0x0000006b | 5 |
| | Row23 | 0x80000035 | 5 |
| | Row22 | 0x400000cf | 7 |
| | Row21 | 0x200000b2 | 5 |
| | Row20 | 0x10000059 | 5 |
| | Row19 | 0x0800002c | 4 |
| | Row18 | 0x04000016 | 4 |
| | Row17 | 0x0200000b | 4 |
| | Row16 | 0x01000005 | 3 |
| | Row15 | 0x008000d7 | 7 |
| | Row14 | 0x0040006b | 6 |
| | Row13 | 0x00200035 | 5 |
| | Row12 | 0x0010001a | 4 |
| | Row11 | 0x000800d8 | 5 |
| | Row10 | 0x000400b9 | 6 |
| | Row9 | 0x00040089 | 4 |
| | Row8 | 0x00020044 | 3 |
| | Row7 | 0x000080f7 | 8 |
| | Row6 | 0x000040ae | 6 |
| | Row5 | 0x00002057 | 6 |
| | Row4 | 0x000010fe | 8 |
| | Row3 | 0x000008aa | 5 |
| | Row2 | 0x00000455 | 5 |
| | Row1 | 0x000002ff | 9 |
| | Row0 | 0x000001aa | 5 |

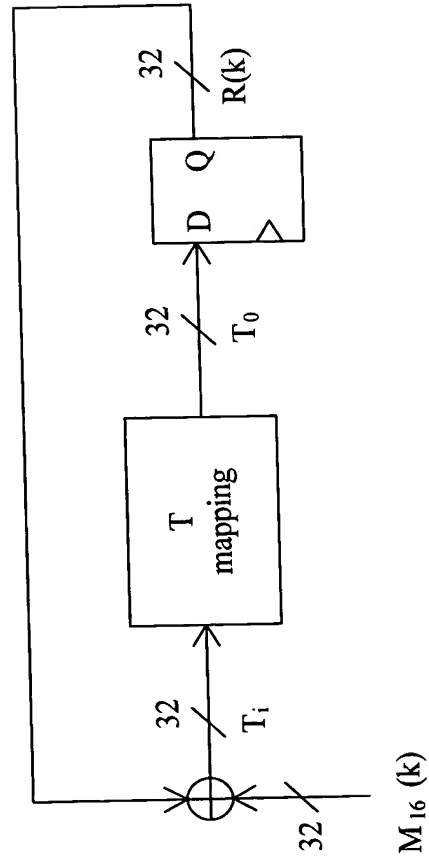
Fig. 5

| | | | | | | | |
|----------------|-------|------------|----|----------------------|-------|------------|----|
| $T = G^{16} =$ | Row31 | 0x8b208000 | 6 | $T^{-1} = G^{-16} =$ | Row31 | 0x0000d558 | 8 |
| | Row30 | 0x45904000 | 6 | | Row30 | 0x00006aac | 8 |
| | Row29 | 0x22c82000 | 6 | | Row29 | 0x00003556 | 8 |
| | Row28 | 0x11641000 | 6 | | Row28 | 0x00001aab | 8 |
| | Row27 | 0x08b20800 | 6 | | Row27 | 0x0000d55 | 7 |
| | Row26 | 0x04590400 | 6 | | Row26 | 0x000006aa | 6 |
| | Row25 | 0x890c0200 | 6 | | Row25 | 0x0000d60d | 8 |
| | Row24 | 0x44860100 | 6 | | Row24 | 0x00006b06 | 7 |
| | Row23 | 0xa2430080 | 7 | | Row23 | 0x00003583 | 7 |
| | Row22 | 0x5a010040 | 6 | | Row22 | 0x0000cf99 | 10 |
| | Row21 | 0x26200020 | 5 | | Row21 | 0x0000b294 | 7 |
| | Row20 | 0x13100010 | 5 | | Row20 | 0x0000594a | 7 |
| | Row19 | 0x89880008 | 6 | | Row19 | 0x00002ca5 | 7 |
| | Row18 | 0xc4c40004 | 7 | | Row18 | 0x00001652 | 6 |
| | Row17 | 0x62620002 | 7 | | Row17 | 0x00000b29 | 6 |
| | Row16 | 0x31310001 | 7 | | Row16 | 0x00000594 | 5 |
| | Row15 | 0x93b80000 | 8 | | Row15 | 0x8000d792 | 10 |
| | Row14 | 0xc9dc0000 | 9 | | Row14 | 0x40006bc9 | 10 |
| | Row13 | 0x64ee0000 | 9 | | Row13 | 0x200035e4 | 9 |
| | Row12 | 0xb2770000 | 10 | | Row12 | 0x10001af2 | 9 |
| | Row11 | 0xd21b0000 | 8 | | Row11 | 0x0800d821 | 7 |
| | Row10 | 0x622d0000 | 7 | | Row10 | 0x0400b948 | 8 |
| | Row9 | 0x3a360000 | 8 | | Row9 | 0x040089fc | 10 |
| | Row8 | 0x1d1b0000 | 8 | | Row8 | 0x010044fe | 10 |
| | Row7 | 0x85ad0000 | 8 | | Row7 | 0x0080f727 | 12 |
| | Row6 | 0x49f60000 | 9 | | Row6 | 0x0040aecb | 11 |
| | Row5 | 0x24fb0000 | 9 | | Row5 | 0x00205765 | 10 |
| | Row4 | 0x995d0000 | 9 | | Row4 | 0x0010feea | 13 |
| | Row3 | 0xc78e0000 | 9 | | Row3 | 0x0008aa2d | 9 |
| | Row2 | 0x63c70000 | 9 | | Row2 | 0x00045516 | 8 |
| | Row1 | 0x3ac30000 | 8 | | Row1 | 0x0002ffd3 | 14 |
| | Row0 | 0x16410000 | 5 | | Row0 | 0x0001aab1 | 9 |

Fig. 6



Scheme 2

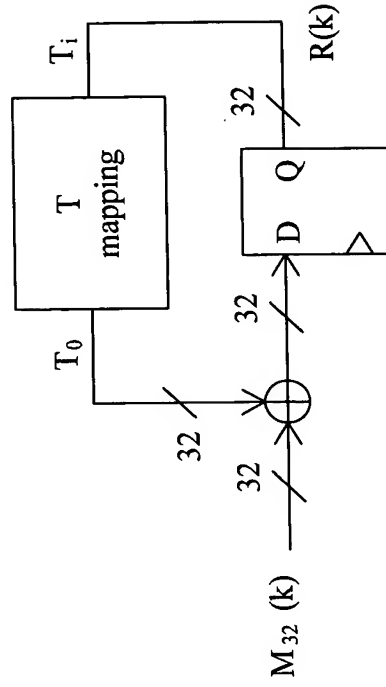


Scheme 1

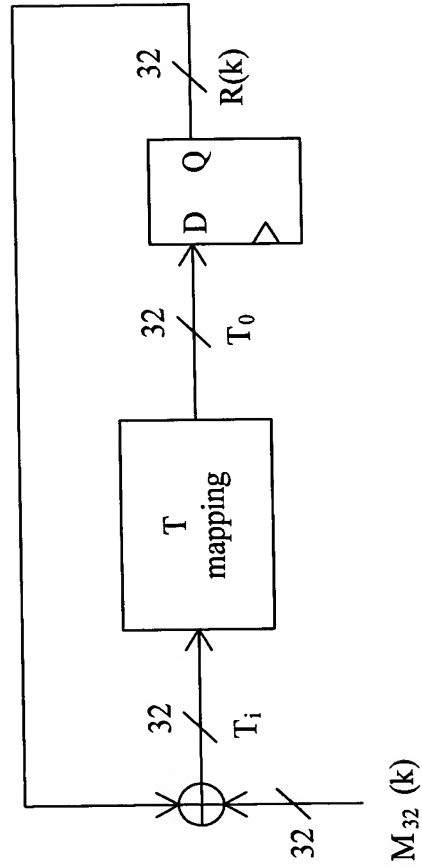
Fig. 7

| | | | | | | | |
|----------------|-------|------------|----|----------------------|-------|------------|----|
| $T = G^{32} =$ | Row31 | 0xfb808b20 | 13 | $T^{-1} = G^{-32} =$ | Row31 | 0xd558a113 | 14 |
| | Row30 | 0x7dc04590 | 13 | | Row30 | 0x6aac5089 | 13 |
| | Row29 | 0xbec022c8 | 14 | | Row29 | 0x35562844 | 12 |
| | Row28 | 0x5f701164 | 14 | | Row28 | 0x1aab1422 | 12 |
| | Row27 | 0x2fb808b2 | 14 | | Row27 | 0x0d558a11 | 12 |
| | Row26 | 0x97dc0459 | 15 | | Row26 | 0x06aac508 | 11 |
| | Row25 | 0xb061890c | 13 | | Row25 | 0xd60dc397 | 17 |
| | Row24 | 0x58374486 | 13 | | Row24 | 0x6b06e1cb | 16 |
| | Row23 | 0xac1ba243 | 14 | | Row23 | 0x358370e5 | 15 |
| | Row22 | 0xad8d5a01 | 14 | | Row22 | 0xcf991961 | 16 |
| | Row21 | 0xad462620 | 12 | | Row21 | 0xb2942da3 | 15 |
| | Row20 | 0x56a31310 | 12 | | Row20 | 0x594a16d1 | 14 |
| | Row19 | 0x2b518988 | 12 | | Row19 | 0x2ca50b68 | 13 |
| | Row18 | 095a8xc4c4 | 13 | | Row18 | 0x165285b4 | 13 |
| | Row17 | 0xcad46262 | 14 | | Row17 | 0x0b2942da | 13 |
| | Row16 | 0x656a3131 | 14 | | Row16 | 0x0594a16d | 13 |
| | Row15 | 0x493593b8 | 15 | | Row15 | 0xd792f1a5 | 18 |
| | Row14 | 0x249ac9dc | 15 | | Row14 | 0x6bc978d2 | 17 |
| | Row13 | 0x924d64ee | 16 | | Row13 | 0x35e4bc69 | 17 |
| | Row12 | 0xc926b277 | 17 | | Row12 | 0x1af25e34 | 16 |
| | Row11 | 0x9f13d21b | 17 | | Row11 | 0xd8218e09 | 12 |
| | Row10 | 0xb409622d | 13 | | Row10 | 0xb9486617 | 15 |
| | Row9 | 0x21843a36 | 12 | | Row9 | 0x89fc9218 | 14 |
| | Row8 | 0x90c21d1b | 13 | | Row8 | 0x44fe490c | 14 |
| | Row7 | 0x33e185ad | 16 | | Row7 | 0xf7278595 | 18 |
| | Row6 | 0x627049f6 | 15 | | Row6 | 0xae6b63d9 | 19 |
| | Row5 | 0x313824fb | 15 | | Row5 | 0x5765b1ec | 18 |
| | Row4 | 0xe31c995d | 17 | | Row4 | 0xf6ea79e5 | 22 |
| | Row3 | 0x8a0ec78e | 15 | | Row3 | 0xaa2d9de1 | 17 |
| | Row2 | 0xc50763c7 | 16 | | Row2 | 0x5516cef0 | 16 |
| | Row1 | 0x19033ac3 | 13 | | Row1 | 0xffd3c66b | 22 |
| | Row0 | 0xf7011641 | 13 | | Row0 | 0xaab14226 | 13 |

Fig. 8



Scheme 2



Scheme 1

Fig. 9